AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Southern District of Ohio

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

SUBJECT DEVICES A THROUGH E, IDENTIFIED IN ATTACHMENT A

Case No. 3:18 mj 457

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Southern District of Ohio, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 922(g)(1)	Felon in Possession of Firearms or Ammunition

The application is based on these facts:

See Attached Affidavit

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Michael Herwig, Special Agent
Printed name and title

Sworn to before me and signed in my presence.

Date: 6/22/18

Judge's signature

City and state: Dayton, Ohio

Michael J. Newman, U.S. Magistrate Judge
Printed name and title

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF SUBJECT DEVICES A THROUGH E, IDENTIFED IN ATTACHMENT A	Case No. _____

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Michael Herwig, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application under Rule 41 of the Federal Rules of Criminal Procedure for a search warrant authorizing the examination of property—electronic devices—which are currently in law enforcement possession, and the extraction from that property of electronically stored information described in Attachment B.

2. I am a Special Agent with the Federal Bureau of Investigation, and have been since March 16, 2008. As a Special Agent, I have been assigned to investigate various Domestic and International Terrorism matters and am assigned to the FBI's Cincinnati Division Joint Terrorism Task Force. These cases have involved the subject's use of cellular telephones and other means of communication. As a Special Agent, I have investigated and analyzed the subject's use of cellular telephones and other means of communication.

3. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

IDENTIFICATION OF THE DEVICES TO BE EXAMINED

4. The property to be searched is as follows (collectively the "SUBJECT DEVICES"), as further described in Attachment A:

a. a black desktop computer, no brand, model, or serial number visible (SUBJECT DEVICE A);

b. an Acer laptop computer, Serial Number LXAZN0Y002902151911601 (SUBJECT DEVICE B);

c. a Systemax desktop computer, Serial Number 106238257 (SUBJECT DEVICE C);

d. a LG Cell Phone, Model K120, Serial Number 608VTBB352133, IMEI: 354873073521330 (SUBJECT DEVICE D);

e. a Black ZTE Cell Phone, Model Z956, Serial Number 320274421041, IMEI: 861170032629072 (SUBJECT DEVICE E).

The SUBJECT DEVICES are currently located at the FBI Dayton Resident Agency, Centerville, Ohio.

5. The applied-for warrant would authorize the forensic examination of the SUBJECT DEVICES for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

6. On March 16, 2018, Affiant became aware of Matthew W. Hetzel (hereinafter HETZEL) when the FBI received a call-in tip that reported threatening statements made by HETZEL. In a follow-up interview, conducted with the reporting party (CHS 1)[1] on the same day, CHS 1 reported to Affiant that HETZEL was in possession of at least several dozen firearms

[1] CHS 1 has provided information to the FBI for less than one year. CHS 1 has a criminal history involving a prior arrest for auto theft. The FBI has not provided any payment to CHS 1.

and many thousands of rounds of ammunition. CHS 1 indicated that HETZEL lived and stored his firearms primarily at his residence, 4495 Infirmary Road, Miamisburg, Ohio, 45342 (hereinafter referred to as PREMISES 1), and that CHS 1 had also seen HETZEL keep several firearms at the auto shop he operated, located in an outbuilding behind 136 W. Main Street, West Carrollton, Ohio (hereinafter referred to as PREMISES 2).

7. On or about March 19, 2018, your Affiant conducted a check of Montgomery County, Ohio, property records for PREMISES 1. The records indicated that the owner of the property was "Hetzell Matthew W," and that the property was purchased on March 16, 2010. On May 11, 2018, your Affiant conducted a check of Montgomery County, Ohio, property records for 136 W. Main Street, West Carrollton, Ohio. The records indicated that the owner of the property was "Kristin M Hetzel." The records also indicated that PREMISES 2 is listed as an outbuilding for this address. On April 26, 2018, your Affiant observed HETZEL exiting PREMISES 2. Additionally, records obtained from Dayton Power & Light show that utility accounts for PREMISES 1 and PREMISES 2 are in the name of Tommie L. Hetzel, HETZEL's wife.

8. On March 19, 2018, your Affiant conducted a query of the criminal history of HETZEL. The query revealed that HETZEL had been convicted on October 17, 1997, of a Felony of the Third Degree for Corrupting Another with Drugs, in violation of Ohio Revised Code § 2925.02(a)(4)(A), which is a crime punishable by imprisonment for a term exceeding one year under Ohio law.

9. On March 22, 2018, CHS 1 reported observing a handgun in PREMISES 2. CHS 1 reported that the gun was located in the drawer of a toolbox. CHS 1 provided a photograph of the gun, which depicts an Arcus brand handgun, silver and black in color, S/N 20DE100401.

10. On March 31, 2018, CHS 1 was at PREMISES 1. CHS 1 observed a gun safe in the corner of the detached garage located just north of the residence. CHS 1 observed that, inside the gun safe, were eight to ten firearms, including both hand guns, and long guns, and one pistol-gripped shotgun.

11. On May 18, 2018, a second FBI confidential human source (CHS 2)[2] met with HETZEL outside of PREMISES 1. During their conversation, which was consensually recorded, CHS 2 and HETZEL began discussing how American citizens own firearms to protect themselves. HETZEL stated, "I don't carry one on me, because it just causes so much trouble nowadays, but anywhere I'm at, especially if I am at home, I'm within 20 feet of one, I'm close enough." HETZEL went on to state, "Both my daughters, their 18th birthday present, when they move out, they each got a shotgun to put in their house. My oldest one just turned 21, I bought her a nine millimeter to carry in her purse, for her 21st birthday."

12. On May 22, 2018, CHS 1 reported to the FBI that on a day in the early months of 2018, CHS 1 met with HETZEL at PREMISES 1. At that time, CHS 1 observed multiple labeled cardboard boxes of .223 ammunition in the bed of HETZEL's vehicle, which was parked in the driveway of PREMISES 1.

13. On May 18, 2018, your Affiant requested and obtained sales records from Aim Surplus, LLC in Monroe, Ohio, a seller of firearms, ammunition and firearms accessories. The records showed on October 28, 2013, Aim Surplus, LLC sold and shipped an order to "Matthew Hetzel, 4495 Infirmary Rd, Miamisburg, OH 45342." The order consisted of twenty (20)

---

[2] CHS 2 has been a FBI source for over 12 years. The CHS has no criminal history. The CHS has been paid approximately $90,000 over the course of 12 years, but has not received any payment related to this investigation.

.223/5.56 magazines with thirty (30) round capacity, and one used Mil. Spec .50 caliber ammunition can. Aim Surplus records indicated the order type was "Ecommerce (AIM website)." An Aim Surplus employee advised the FBI that "Ecommerce" indicates that HETZEL conducted the purchase online rather than coming to the store.

14. On May 29, 2018, the Honorable Sharon L. Ovington, United States Magistrate Judge for the Southern District of Ohio, issued search warrants authorizing the search of PREMISES 1 and PREMISES 2. The search warrants authorized the seizure of Electronic devices that can access the internet, including but not limited to desktop computers, laptops, iPads, tablets, cellular telephones, digital video recording devices and storage media, and any attached storage devices such as thumb drive, external hard drives, CD's, DVD's and SD cards.

15. On May 30, 2018, the FBI executed the search warrants for PREMISES 1 and PREMISES 2. As a result of the execution of these search warrants, the FBI seized 145 firearms, and ammunition estimated to be in excess of 10,000 rounds. Additionally, the following electronic items were seized pursuant to the search warrants:

a. A Black ZTE Cell Phone, Model Z956, Serial Number 320274421041, IMEI: 861170032629072 (SUBJECT DEVICE E), which was recovered from beside the bed in HETZEL's bedroom in PREMISES 1. During a FBI interview on May 30, 2018, HETZEL stated his phone was a ZTE model and was located next to his bed.

b. Acer laptop computer, Serial Number LXAZN0Y002902151911601 (SUBJECT DEVICE B), which was recovered in a gun safe which also contained firearms and ammunition in PREMISES 1.

c. Systemax desktop computer, Serial Number 106238257 (SUBJECT DEVICE C), recovered in the main living area of the house in PREMISES 1. During a FBI interview on May 30, 2018, HETZEL stated he utilized the desktop computer located in his living room.

d. Black desktop computer, no brand, model, or serial number visible (SUBJECT DEVICE A), found near a desk in PREMISES 2.

e. LG Cell Phone, Model K120, Serial Number 608VTBB352133, IMEI: 354873073521330 (SUBJECT DEVICE D), located in the drawer of a tool chest at PREMISES 2.

16. During FBI interviews of Matthew W. Hetzel, and his wife, Tommie Hetzel, conducted on May 30, 2018, both stated that Matthew Hetzel utilized the ZTE cell phone (SUBJECT DEVICE E) and the Systemax desktop computer (SUBJECT DEVICE C). Additionally, Tommie Hetzel claimed to have no knowledge of the Acer laptop (SUBJECT DEVICE B), which was located in a gun safe along with firearms and ammunition. Both the unlabeled black desktop computer (SUBJECT DEVICE A), and the LG K120 cell phone (SUBJECT DEVICE D), were located in the workplace of Matthew W. Hetzel, among other property belonging to Hetzel.

17. The SUBJECT DEVICES are currently in the lawful possession of the FBI. They came into the FBI's possession pursuant to authorization to seize electronic items in federal search warrants issued for PREMISES 1 and PREMISES 2. Therefore, while the FBI might already have all necessary authority to examine the SUBJECT DEVICES, I seek this additional warrant out of an abundance of caution to be certain that an examination of the SUBJECT DEVICES will comply with the Fourth Amendment and other applicable laws.

18. The SUBJECT DEVICES are currently in storage at the FBI Dayton Resident Agency in Centerville, Ohio. In my training and experience, I know that the SUBJECT DEVICES have been stored in a manner in which their contents are, to the extent material to this investigation, in substantially the same state as they were when the SUBJECT DEVICES first came into the possession of the FBI.

TECHNICAL TERMS

19. Based on my training and experience, I use the following technical terms to convey the following meanings:

a. Wireless telephone: A wireless telephone (or mobile telephone, or cellular telephone) is a handheld wireless device used for voice and data communication through radio signals. These telephones send signals through networks of transmitter/receivers, enabling communication with other wireless telephones or traditional "land line" telephones. A wireless telephone usually contains a "call log," which records the telephone number, date, and time of calls made to and from the phone. In addition to enabling voice communications, wireless telephones offer a broad range of capabilities. These capabilities include: storing names and phone numbers in electronic "address books;" sending, receiving, and storing text messages and e-mail; taking, sending, receiving, and storing still photographs and moving video; storing and playing back audio files; storing dates, appointments, and other information on personal calendars; and accessing and downloading information from the Internet. Wireless telephones may also include global positioning system ("GPS") technology for determining the location of the device.

b. Digital camera: A digital camera is a camera that records pictures as digital picture files, rather than by using photographic film. Digital cameras use a variety of fixed and removable storage media to store their recorded images. Images can usually be retrieved by connecting the camera to a computer or by connecting the removable storage medium to a separate reader. Removable storage media include various types of flash memory cards or miniature hard drives. Most digital cameras also include a screen for viewing the stored images. This storage media can contain any digital data, including data unrelated to photographs or videos.

c. Portable media player: A portable media player (or "MP3 Player" or iPod) is a handheld digital storage device designed primarily to store and play audio, video, or photographic files. However, a portable media player can also store other digital data. Some portable media players can use removable storage media. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can also store any digital data. Depending on the model, a portable media player may have the ability to store very large amounts of electronic data and may offer additional features such as a calendar, contact list, clock, or games.

d. GPS: A GPS navigation device uses the Global Positioning System to display its current location. It often contains records the locations where it has been. Some GPS navigation devices can give a user driving or walking directions to another location. These devices can contain records of the addresses or locations involved in such navigation. The Global Positioning System (generally abbreviated

"GPS") consists of 24 NAVSTAR satellites orbiting the Earth. Each satellite contains an extremely accurate clock. Each satellite repeatedly transmits by radio a mathematical representation of the current time, combined with a special sequence of numbers. These signals are sent by radio, using specifications that are publicly available. A GPS antenna on Earth can receive those signals. When a GPS antenna receives signals from at least four satellites, a computer connected to that antenna can mathematically calculate the antenna's latitude, longitude, and sometimes altitude with a high level of precision.

e. PDA: A personal digital assistant, or PDA, is a handheld electronic device used for storing data (such as names, addresses, appointments or notes) and utilizing computer programs. Some PDAs also function as wireless communication devices and are used to access the Internet and send and receive e-mail. PDAs usually include a memory card or other removable storage media for storing data and a keyboard and/or touch screen for entering data. Removable storage media include various types of flash memory cards or miniature hard drives. This removable storage media can store any digital data. Most PDAs run computer software, giving them many of the same capabilities as personal computers. For example, PDA users can work with word-processing documents, spreadsheets, and presentations. PDAs may also include global positioning system ("GPS") technology for determining the location of the device.

f. Tablet: A tablet is a mobile computer, typically larger than a phone yet smaller than a notebook, that is primarily operated by touching the screen. Tablets function as wireless communication devices and can be used to access the Internet

through cellular networks, 802.11 "wi-fi" networks, or otherwise. Tablets typically contain programs called apps, which, like programs on a personal computer, perform different functions and save data associated with those functions. Apps can, for example, permit accessing the Web, sending and receiving e-mail, and participating in Internet social networks.

g. IP Address: An Internet Protocol address (or simply "IP address") is a unique numeric address used by computers on the Internet. Every computer attached to the Internet computer must be assigned an IP address so that Internet traffic sent from and directed to that computer may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static—that is, long-term—IP addresses, while other computers have dynamic—that is, frequently changed—IP addresses.

h. Internet: The Internet is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

20. Based on my training, experience, and research, I know that the SUBJECT DEVICES A, B, and C have capabilities that allow them to serve as a computer, a digital camera, a means to access the internet, and as a phone to make internet calls. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

21. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.zteusa.com, I know that SUBJECT DEVICE E has capabilities that allow it to serve as a wireless telephone, digital camera, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

22. Based on my training, experience, and research, and from consulting the manufacturer's advertisements and product technical specifications available online at http://www.lg.com, I know that SUBJECT DEVICE D has capabilities that allow it to serve as a computer, a wireless telephone, digital camera, a means to access the internet, and as a phone to make internet calls, portable media player, GPS navigation device, and PDA. In my training and experience, examining data stored on devices of this type can uncover, among other things, evidence that reveals or suggests who possessed or used the device.

23. Based on my training and experience, I know that individuals who are involved in the purchase of firearms and ammunition, including those who are prohibited from possessing these items, often use cellular telephones, computers, and/or the internet to purchase or exchange these items. As discussed above in paragraph 13, records from Aim Surplus, LLC indicate that HETZEL purchased ammunition magazines and an ammunition can using an online system.

ELECTRONIC STORAGE AND FORENSIC ANALYSIS

24. Based on my knowledge, training, and experience, I know that electronic devices can store information for long periods of time. Similarly, things that have been viewed via the Internet are typically stored for some period of time on the device. This information can sometimes be recovered with forensics tools.

25. There is probable cause to believe that things that were once stored on the SUBJECT DEVICES may still be stored there, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer's operating system may also keep a record of deleted data in a "swap" or "recovery" file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or "cache."

26. *Forensic evidence.* As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the SUBJECT DEVICES were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence might be on the SUBJECT DEVICES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created.

b. Forensic evidence on a device can also indicate who has used or controlled the device. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. A person with appropriate familiarity with how an electronic device works may, after examining this forensic evidence in its proper context, be able to draw conclusions about how electronic devices were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact electronically stored information on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Electronic evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium.

27. *Nature of examination.* Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit the examination of the SUBJECT DEVICES consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the devices to human inspection in order to determine whether it is evidence described by the warrant.

28. *Manner of execution.* Because this warrant seeks only permission to examine devices already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premises. Consequently, I submit there is reasonable cause for the Court to authorize execution of the warrant at any time in the day or night.

CONCLUSION

29. Based on the aforementioned factual information, I respectfully submit that there is probable cause to believe that evidence, fruits, and instrumentalities of violations of federal

law, including 18 U.S.C. § 922(g), are present within the information located on the SUBJECT DEVICES described in Attachment A. I, therefore, respectfully request that attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

REQUEST FOR SEALING

30. It is respectfully requested that this Court issue an order sealing, until further order of the Court, all papers submitted in support of this application, including the application and search warrant. I believe that sealing this document is necessary because the warrant is relevant to an ongoing investigation. Premature disclosure of the contents of this affidavit and related documents may have a significant and negative impact on the continuing investigation and may severely jeopardize its effectiveness.

Respectfully submitted,

Michael Herwig
Special Agent
Federal Bureau of Investigation

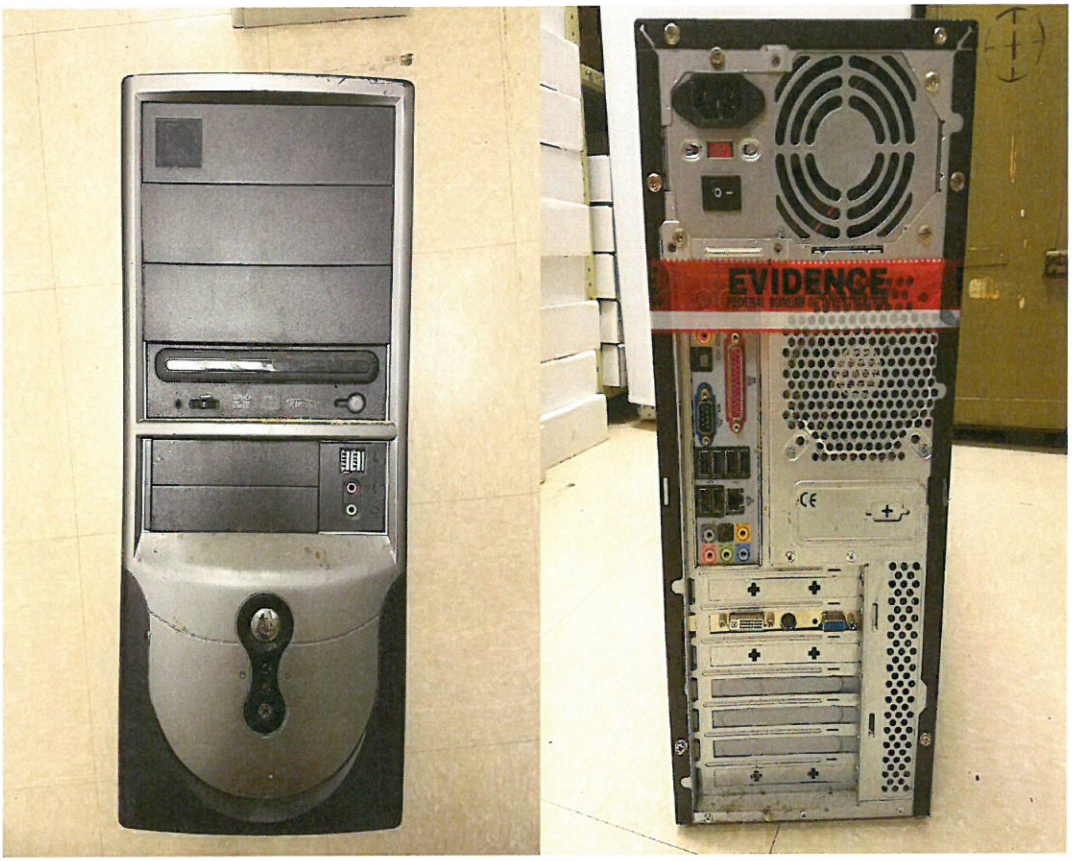
Subscribed and sworn to before me on June 22, 2018.

MICHAEL J. NEWMAN
UNITED STATES MAGISTRATE JUDGE

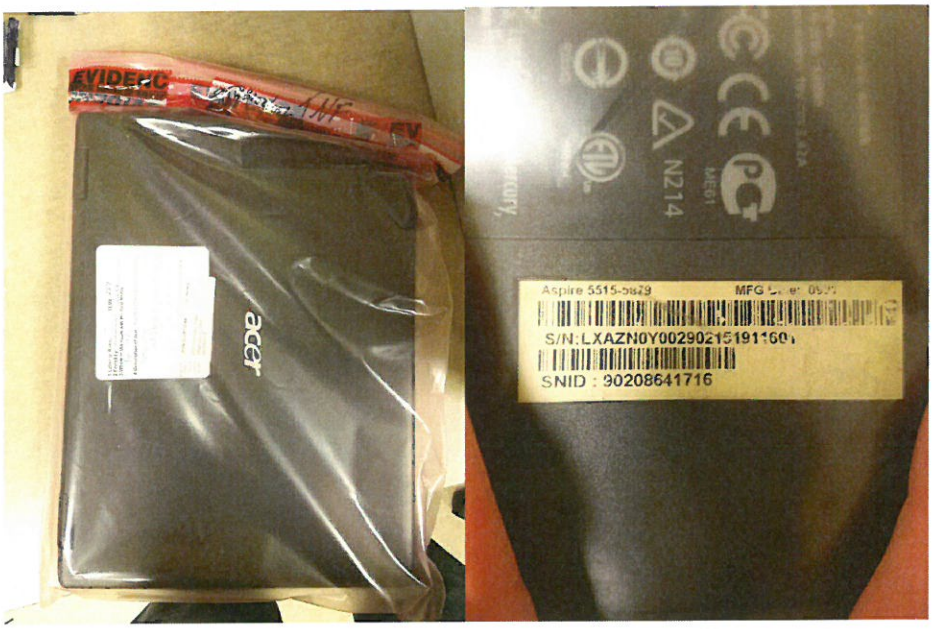
ATTACHMENT A

The property to be searched are the following SUBJECT DEVICES A through E, which are currently located at the FBI Dayton Resident Agency, Centerville, Ohio. This warrant authorizes the forensic examination of SUBJECT DEVICES A through E for the purpose of identifying the electronically stored information described in Attachment B.

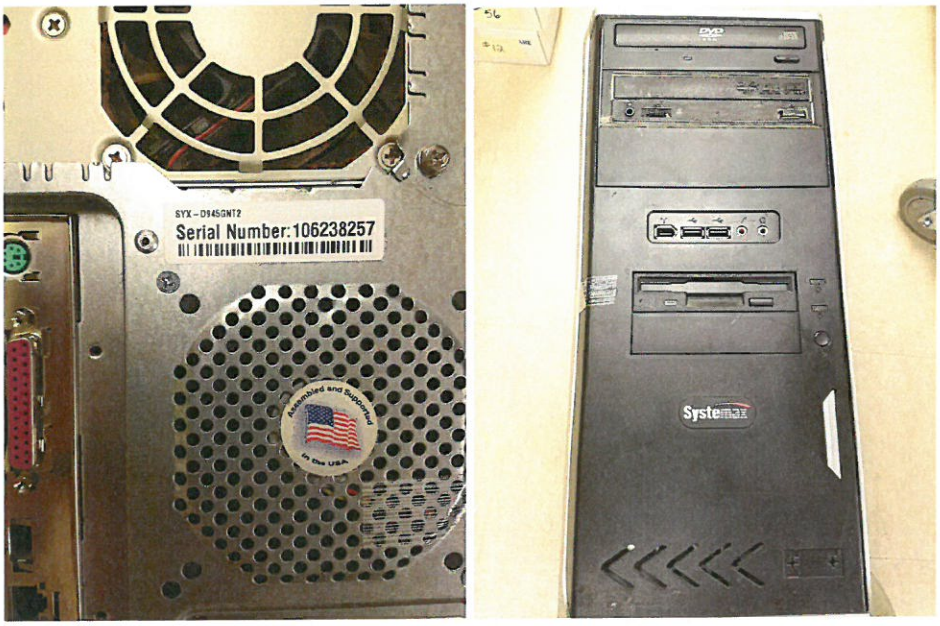
1. **SUBJECT DEVICE A**: The property to be searched is a black desktop computer, no brand, model, or serial number visible. Photographs of SUBJECT DEVICE A are below.



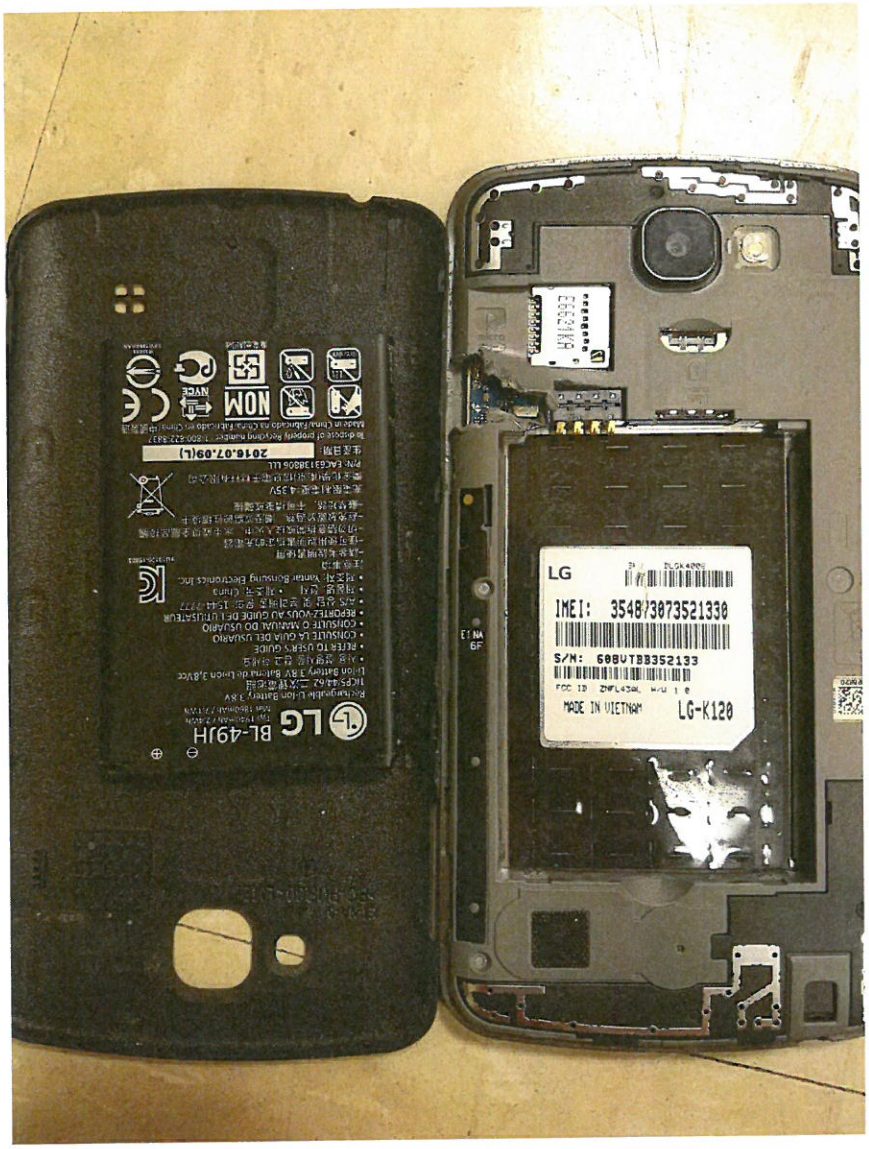
2. **SUBJECT DEVICE B**: The property to be searched is an Acer laptop computer, Serial Number LXAZN0Y002902151911601. Photographs of SUBJECT DEVICE B are below.



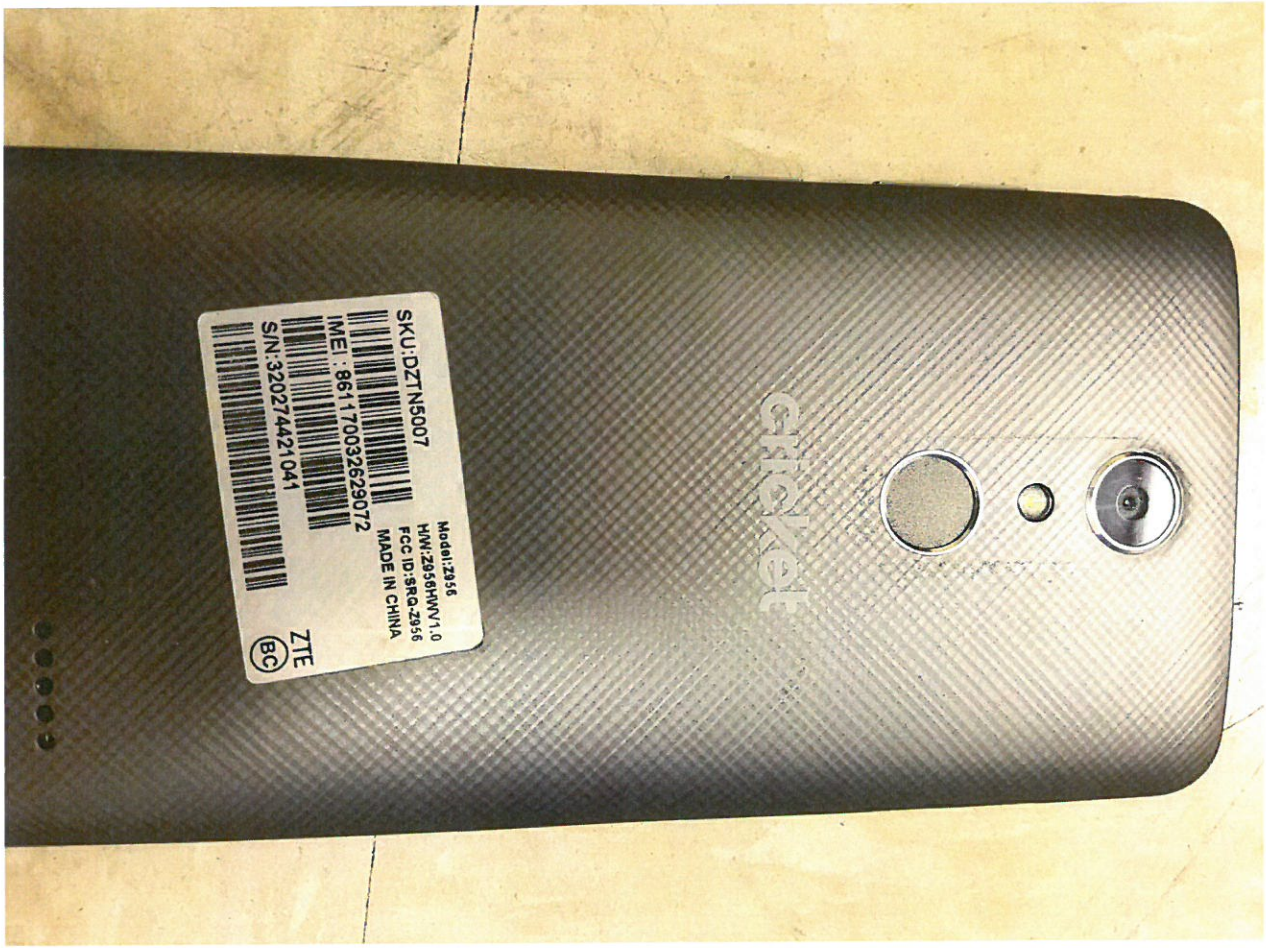
3. **SUBJECT DEVICE C**: The property to be searched is a Systemax desktop computer, Serial Number 106238257. Photographs of SUBJECT DEVICE C are below.



4. **SUBJECT DEVICE D**: The property to be searched is a LG Cell Phone, Model K120, Serial Number 608VTBB352133, IMEI: 354873073521330. A photograph of SUBJECT DEVICE D is below.



5. **SUBJECT DEVICE E**: The property to be searched is a Black ZTE Cell Phone, Model Z956, Serial Number 320274421041, IMEI: 861170032629072. A photograph of SUBJECT DEVICE E is below.



ATTACHMENT B

All records on SUBJECT DEVICES A through E described in Attachment A that relate to violations of Title 18 U.S.C. § 922(g)(1) and involve Matthew W. Hetzel, including:

a. Electronic logs, records, payment receipts, notes, photos, videos, customer lists, ledgers, records, or communications relating to the transportation, ordering, purchasing, and/or sale of firearms, and/or ammunition;

b. Electronic addresses and/or telephone books and papers reflecting names, e-mail and physical addresses and/or telephone numbers of individuals, partnerships, or corporations involved in the purchasing or selling of firearms to/from prohibited persons;

c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

d. any information related to Internet Protocol (IP) addresses and Wi-Fi accounts accessed by the device;

e. any GPS information on the device;

f. all bank records, checks, credit card bills, account information, and other financial records;

g. Evidence of user attribution showing who used or owned the device at the time the things described in this warrant were created, edited, or deleted, such as logs, phonebooks, saved usernames and passwords, documents, and browsing history.

As used above, the terms "records" and "information" include all of the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including any form of computer or electronic storage (such as flash memory or other media that can store data) and any photographic form.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.